REMARKS/ARGUMENTS

Claims 1-6, 9-25, and 27-32 are pending. Claims 1, 9, and 15 have been amended. No new matter has been introduced. Applicant believes the claims comply with 35 U.S.C. § 112.

Applicants note with appreciation the allowance of claims 21-25 and 30-32.

Applicant would like to thank Examiner Joseph Pan and Supervisory Patent Examiner Thanhnga B. Truong for the courteous telephone interview extended to Applicant's counsel, Chun-Pok Leung, on April 19, 2006. During the interview, proposed amendments that would place the application in better condition for allowance were discussed. *It was reiterated that the cited references do not teach or suggest accessing (processing read/write request of data) during converting (encrypting/decrypting of data).*

The claims have been amended accordingly. More specifically, claim 1 has been amended to recite "receiving and processing a read request during said converting in order to access read data from said storage system." Claim 9 has been amended to recite "accessing read data from said storage device . . . wherein said third data block is one of said plurality of second data blocks." Claim 15 has been amended to recite "wherein said cryptographic component is further operable to receive and process read and write requests for data stored on said storage component."

Claims 1-4, 6, 9-17, 20, and 27-29 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Bojinov et al. (US 2005/0102498). Claim 5 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Bojinov et al. in view of Ashton (US 2004/0125077). The Examiner recognizes that Bojinov et al. does not teach that encrypting and decrypting are performed on the logic circuitry, and cites Ashton for allegedly disclosing the missing feature. Claims 18 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Bojinov et al. in view of Cane et al. (US 5,940,507). The Examiner cites Cane et al. for allegedly disclosing a cryptographic engine for encrypting a file.

Claims 1-6 and 27-29

Applicant respectfully submits that independent claim 1 is novel and patentable over Bojinov et al. because, for instance, Bojinov et al. does not teach or suggest receiving and processing a read request during converting blocks of data to produce converted blocks of data in order to access read data from the storage system, and in response thereto accessing the read data from at least one decrypted block of data, wherein the read data is decrypted from one converted block of the converted blocks of data using the cryptographic criteria to produce the at least one decrypted block of data. In other words, a portion of the converted blocks of data is accessed (after being decrypted) while the blocks of data are being converted to produce the converted blocks of data (by encryption). The accessing and the converting of the data occur in parallel.

Applicant notes that support for the feature of "wherein said read data is decrypted from one converted block of said converted blocks of data using said cryptographic criteria to produce said at least one decrypted block of data" can be found, for example, in Fig. 3 and paragraphs [31]-[33] at page 8. More specifically, a converted block of data is decrypted using either first cryptographic criteria 106 in block 305 or second cryptographic criteria 107 in block 304 to produce a decrypted block of data.

In contrast, the writing/reading and the encrypting/decrypting of data in Bojinov et al. occur in series. There is no parallel processing of writing/reading and encrypting/decrypting of the data. More specifically, there is **no** processing of a read request during converting of data, as recited in claim 1. Ashton does not cure the deficiencies of Bojinov et al.

For at least the foregoing reasons, claim 1, and claims 2-6 and 27-29 depending therefrom, are patentable.

Claims 9-14

Applicant respectfully submits that independent claim 9 is novel and patentable over Bojinov et al. because, for instance, Bojinov et al. does not teach or suggest accessing read data from the storage device in response to a read request from the host device, including reading a third data block and decrypting the third data block with the

cryptographic criteria wherein the third data block is one of the plurality of second data blocks, to return the decrypted third data block to the host device, wherein the step of accessing read data is performed during the step of converting. In other words, a portion of the plurality of second data blocks is accessed (after being decrypted as the third data block) while a plurality of first data blocks are being converted to produce the plurality of second data blocks (by encryption). The accessing and the converting of the data occur in parallel.

In contrast, the writing/reading and the encrypting/decrypting of data in Bojinov et al. occur in series. There is no parallel processing of writing/reading and encrypting/decrypting of the data. More specifically, there is **no** accessing of read data during converting of data, as recited in claim 9.

For at least the foregoing reasons, claim 9 and claims 10-14 depending therefrom are patentable.

Claims 15-20

Applicant respectfully submits that independent claim 15 is novel and patentable over Bojinov et al. because, for instance, Bojinov et al. does not teach or suggest a cryptographic component that is operable to receive and process read and write requests for data stored on the storage component, while the plurality of unconverted blocks of data are converted to the plurality of converted blocks of data, wherein the cryptographic component is further operable to process a read request by accessing read blocks associated with the read request from the storage component, wherein if a read block is one of the unconverted blocks of data, then performing a first cryptographic process on the read block to produce an unencrypted read block, wherein if the read block is one of the converted blocks of data, then performing a second cryptographic process on the read block to produce an unencrypted read block, and wherein the cryptographic component is further operable to process a write request by writing one or more write blocks associated with the write request from the storage component, wherein if a write block is to be written to a block location that contains an unconverted block, then performing the first cryptographic process on the write block prior to writing the write block, wherein if a write block is to be written to a block location that

contains a converted block, then performing the second cryptographic process on the write block prior to writing the write block.

In other words, for a read request, if a read block to be accessed is one of the unconverted blocks of data, a portion of the plurality of unconverted blocks is accessed (after being decrypted as the unencrypted read block using a first cryptographic process) while the plurality of unconverted blocks of data are being converted to a plurality of converted blocks of data (by encryption); or, if a read block to be accessed is one of the converted blocks of data, a portion of the plurality of converted blocks of data is accessed (after being decrypted as the unencrypted read block using a second cryptographic process) while the plurality of unconverted blocks of data are being converted to a plurality of converted blocks of data (by encryption). The accessing and the converting of the data occur in parallel.

For a write request, if a write block is to be written to a block location that contains one of the unconverted blocks of data, the write block is written (after being processed using the first cryptographic process); or, if a write block is to be written to a block location that contains one of the converted blocks of data, the write block is written (after being processed using the second cryptographic process). The writing and the converting of the data occur in parallel.

In contrast, the writing/reading and the encrypting/decrypting of data in Bojinov et al. occur in series. There is no parallel processing of writing/reading and encrypting/decrypting of the data. More specifically, there is **no** processing of read and write requests while blocks of data are converted, as recited in claim 15. Cane et al. does not cure the deficiencies of Bojinov et al.

For at least the foregoing reasons, claim 15 and claims 16-20 depending therefrom are patentable.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

Chun-Pok Leung
Reg. No. 41,405

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
RL:rl
60752710 v1